网络系统安全

WANG LUO XI TONG AN QUAN

主　编：张来顺

WANG LUO XI TONG AN QUAN

WANG LUO XI TONG AN QUAN

解放军出版社

前　言

为积极推进中国特色军事变革，加速军队信息化建设，培养高素质军事人才，我们组织军队有关专家、学者编写了《网络系统安全》一书。

本书主要介绍了网络系统安全的基本概念、基本原理和基本方法。重点对防火墙技术、入侵检测技术、黑客攻击与防御、网络病毒与防范、安全审计与风险评估等内容作了阐述和分析。

本书可列为部队机关、军事院校以及自学考试、电大考试选用教材或教学参考书，也可作为部队官兵系统学习信息技术知识的教科书。

总参政治部宣传部

二〇〇五年五月

目　录

第一章　计算机网络基础知识

随着计算机技术的飞速发展，计算机的应用已渗透到社会的各个领域。社会的信息化、数据的分布处理以及各种计算机资源的共享等要求，推动着计算机技术朝着群体化的方向发展，使人们从单机操作扩大到网上操作，以共享网上的巨大资源，并方便地实现与网上其他用户的信息交流。计算机网络由最初的主机一终端模式，逐步发展成为基于多种协议的局域网和广域网，现在则是以 Internet 为代表的国际互联网。Internet 将全世界的计算机连接在一起，使人们上网交流和共享信息资源等更为方便。Internet 正在广泛地影响现代生活的各个方面。

本章主要介绍与网络系统安全关系紧密的相关计算机网络基础知识。

第一节　计算机网络的概念

一、计算机网络的定义

计算机网络是计算机与通信这两大现代技术紧密结合的产物，它代表着当前计算机体系结构发展的一个重要方面。计算机只有和网络相结合，才能发挥更强大的作用。

所谓计算机网络，是将分散在不同地点的计算机和计算机系统，通过通信设备和线路连接起来，在网络软件（即网络通信协议、信息交换方式及网络操作系统等）的支持下进行数据通信，以实现资源共享的计算机系统。

二、计算机网络的功能

计算机网络的功能很多，主要功能有资源共享、信息交换、分布式处理及网络管理等几个方面。

（一）资源共享

资源共享是计算机联网的主要目的，共享的资源包括硬件、软件、数据和信息。

1. 软件资源共享。软件资源包括各种语言、服务程序、应用程序和工具，通过联网可以实现软件资源共享。

2. 硬件资源共享。网上用户还可以共享网上的硬件设备，特别是一些特殊设备或价格昂贵的设备，如大型主机、高速打印机、海量存储器等。

3. 信息资源共享。网上用户可以使用网上公共数据库中的信息。数据库可以集中设置，也可以分布在多个节点上。随着Internet的发展，网上的信息服务正成为一种新的服务行业而蓬勃发展。连入Internet上的用户，可以享受全球范围的资料检索、信息发布、电子邮件等多种服务。

（二）信息交换

信息交换是指通过计算机网络完成网络中各个节点之间的数据传送，它是实现其他功能的基础。用户可以在网上传送电子邮件、发布新闻消息、进行电子购物、远程教育等。

（三）分布式处理

在网络的支持下，可以将某些大型处理任务转化成小型任务而由网络中的各计算机分布处理，即多个系统协同工作，均衡负荷，共同完成某一处理工作。

（四）网络管理

计算机网络是开放性的系统，适应网络中多个用户之间的交往。连入网络中的计算机系统，不仅能使用本机所具有的各种资源，而且也应能通过网络使用网中其他的资源。这就要求有一个

对整个网络进行统一、合理的管理方法，保证网络中通信功能的正常实施。网络管理主要是从通信接口和通信控制两方面进行管理。

（五）办公自动化

一个现代意义的办公自动化系统并不是一些零散先进设备和机器的组合，它是一个完整的软件和硬件设备的集合，并通过一个网络系统形成一个较为全面的控制过程。一个比较完整的办公自动化系统应当包括信息采集、信息处理、信息传送、信息存储这四个基本环节，并能实现资源共享。在这里，信息的传送是在网络上进行的，通过网络的管理功能，可以实现各个部门之间的有序操作，大大提高工作效率和管理水平。

三、计算机网络的组成

计算机网络由两个基本部分组成，即通信子网和资源子网，如图 1－1 所示。

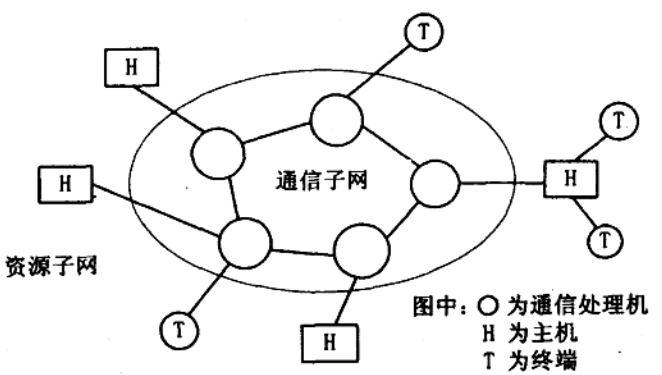

图 1－1　计算机网络一般结构

（一）通信子网

通信子网负责数据传输、交换及通信控制，它包含物理信道和通信设备。物理信道是用来传输数据的传输介质，可以是双绞线、同轴电缆、光缆，也可以是市话线、长话线等。物理信道除采用有线外，还可以是无线信道，如微波和卫星通信等。

通信设备可以是通信处理机及各种交换设备。在局域网中，通信处理机（也称网络适配器或网卡）是主机与网络的接口，数据通过通信处理机后在传输介质上传送，通信处理机负责数据转接、路径选择等通信处理任务。

（二）资源子网

资源子网负责全网的数据处理和向网络用户提供网内可共享的资源及网络服务等。资源子网一般由主计算机系统、终端、各种软件资源和数据资源等组成。

四、计算机网络的分类

计算机网络的分类方法很多，这里给出按照网络的分布距离及网络的拓扑结构来分类的方法。

（一）按分布距离分类

按照分布距离的长短，计算机网络可分为局域网 LAN（Local Area Network）、广域网 WAN（Wide Area Network）和互联网（Internet）。

1. 局域网

局域网的地理分布范围比较小，一般在十几公里以内。它是一个部门或单位组建的计算机网络，如建立在一座建筑物内或一个校园内的网络。局域网具有成本低、传输速率高、延迟小、组网方便、使用灵活等特点。局域网主要有三种网络拓扑结构，即总线结构、环形结构和星形结构。目前流行的局域网为星形结构的以太网。

2. 广域网

广域网的分布范围较大，可以实现一个城市乃至一个国家的计算机网络互联。广域网的网络规模大，提供的资源丰富，可以实现远程计算机通信，更能发挥计算机网络的优势。但由于广域网距离远，架设专门的通信线路较为困难，经常租用电话或微波等通信线路，因此通信费用较高。而且由于一般邮电通信线路带宽较窄，所以其传输速率比局域网要低得多。

目前有几个全国范围的计算机网络就属于这类网络，如 Chinanet、CERnet 等。

3. 国际互联网

互联网其实并不是一种单独规划和建造的网络，而是将已有的不同物理网络按照某种协议连接起来，实现网络与网络之间的通信。比如将局域网与局域网、局域网与广域网、广域网与广域网进行互联，实现局部处理与远程处理、有限地域范围资源共享与广大地域范围资源共享相结合的互联网。目前世界上最大的互联网是 Internet。

（二）按网络拓扑结构分类

将多个独立的计算机系统连成网络有多种连接方法，我们把组成网络的各个节点之间的连接方式称为拓扑结构。计算机网络的拓扑结构主要有下列五种：

1. 总线结构

总线结构网络采用一条开环、无源的双绞线或同轴电缆，通过相应的接口把所有计算机设备均连接到该电缆上，形成一条公共的多路访问总线。总线上的任何一台主机都是平等的，一个节点发送的信号其他节点均可接收。总线的拓扑结构如图 1－2（a）所示。

总线结构常用于局域网，其特点是网络结构简单，在总线上增减设备容易，扩充性好，但总线本身的故障将导致网络的瘫痪。

2. 环形结构

在环形网络结构中，各个节点首尾相接构成了一个封闭的环，如图1－2（b）所示。信号通常是顺着一个方向从一台主机传到另一台主机，每台主机在向内来的电缆上都有一个接收器，在向外去的电缆上都有一个发送器。环上每个节点都是平等的，均可向其他节点发送信息。

环形结构的网络常用于局域网。其特点是数据沿环路依次传递，信息延迟是稳定的和可预测的。其缺点是当某个节点发生故障时，会影响到整个网络的工作。

3. 星形结构

星形结构以一个特定节点为中心，从中心以辐射状线路连接到其他节点，如图1－2（c）所示。这个中心节点所用设备一般为集线器。

在星形结构的网络中，任意一条线路的损坏只会影响到与该线路相连的一个节点设备，而对其他节点设备的工作无影响。因此，这是一种比较稳定可靠的拓扑结构。

4. 树形结构

如果将星形网络中的普通节点用作另一个星形网络的中心节点，就构成了树形网络，如图1－2（d）所示。因此，树形结构是星形结构的扩充，具有与星形网络相似的特点。

5. 分布式结构

分布式网络结构是由分布在不同地点且具有多个终端的节点互连而成的，如图1－2（e）所示。在该网络中，任一节点至少与两条线路相连，当任意一条线路发生故障时，通信可转经其他链路完成，因而具有较高的可靠性。同时，分布式网络易于扩充。缺点是网络控制机构复杂，线路增多时成本会增加。

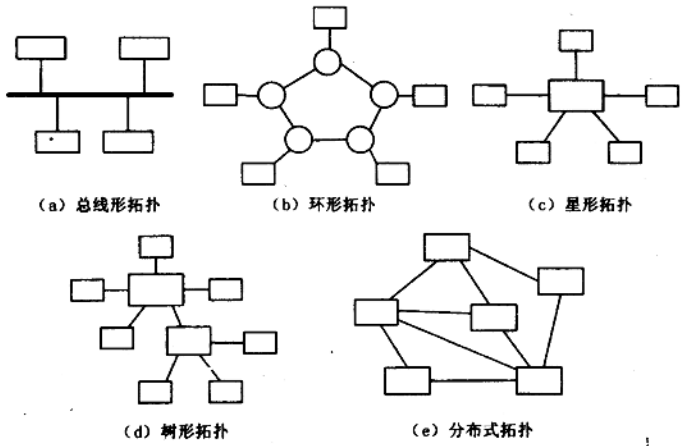

图 1-2　网络的拓扑结构

第二节　计算机网络体系结构

建立计算机网络的目的是为了共享网内资源和交换信息。由于网内的计算机系统及设备各不相同，彼此间要进行通信，就必须遵守共同的规则和约定，这种规则和约定就是通信协议。

对于一个网络系统及其组成部件（包括硬件、软件和通信线路）的功能描述与定义，称之为网络的体系结构。网络体系结构描述的是各个部分之间的逻辑连接及信息流程，不涉及具体的硬件及软件组成。

一、OSI 参考模型

国际标准化组织（ISO）是世界上最著名的国际性标准化组织之一。ISO 于 1977 年建立了计算机网络标准分委员会，负责

研究网络的标准化问题。该委员会于 1982 年提出了一个网络体系结构的七层参考模型，即 OSI（开放系统互联）参考模型。该模型已被世界各国所承认。参照 OSI 模型进行标准化，就使得各系统之间能够互联，并最终开发成全球的网络结构。

OSI 参考模型的主要特征如下：

1. OSI 是一种将异种系统互连的分层结构，提供了控制互连系统交互规则的标准框架，定义了抽象结构而并非具体实现的描述；

2. 对等层之间的通信必须遵循相应层的协议，如网络层协议、传输层协议等；

3. 相邻层之间的接口定义了原语操作和低层向上层提供的服务；

4. 所提供的公共服务是面向连接的或无连接的数据通信服务。

OSI 参考模型的结构如图 1－3 所示。OSI 共划分为七层，每一层都具有一定的独立性，它们各自完成各自的任务，依靠各层的功能组合就可以提供访问通路。

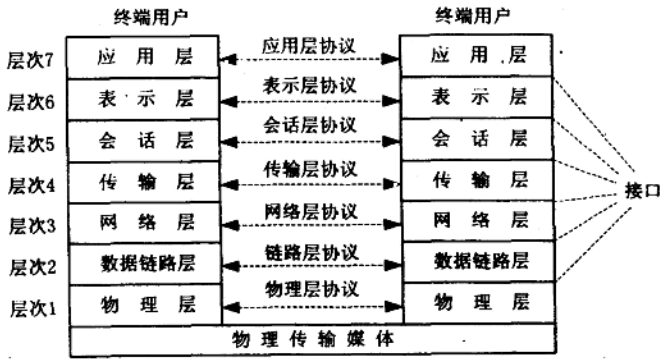

图 1－3　OSI 参考模型的结构

在七层结构中，每一层都为上一层提供服务。因此，越向上层其功能越具综合性和宏观控制特性，下层承担具体的基础工作。通信时，数据从上层逐层传递到下层，在物理层连接到通道的物理介质上，完成通信。接收方则将物理层的数据依次向上传递，方向与发送方相反。在这七层中，1～4 层为低层，设计为面向通信的；5～7 为高层，是面向信息处理的。

划分为层次后，可以使层间的接口更加标准化，由于各层相对独立，易于变更和扩充。各层次需要解决层间的服务规范和层内的通信协议规范。

各层的基本功能说明如下：

1. 物理层

在 OSI 参考模型中，物理层（Physical Layer）是参考模型的最低层。物理层的主要功能是：利用传输介质为通信的网络节点之间建立、管理和释放物理连接，实现比特流的透明传输，为数据链路层提供数据传输服务。物理层的数据传输单元是比特（bit）。

2. 数据链路层

在 OSI 参考模型中，数据链路层（Data Link Layer）是参考模型的第 2 层。数据链路层的主要功能是：在物理层提供的服务基础上，数据链路层在通信的实体间建立数据链路连接，传输以帧为单位的数据包，并采用差错控制与流量控制方法，使有差错的物理线路变成无差错的数据链路。

3. 网络层

在 OSI 参考模型中，网络层（Network Layer）是参考模型的第 3 层。网络层的主要功能是：通过路由选择算法为分组通过通信子网选择最适当的路径，以及实现拥塞控制、网络互联等功能。网络层的数据传输单元是分组（packet）。

4. 传输层

在 OSI 参考模型中，传输层（Transport Layer）是参考模型的第 4 层。传输层的主要功能是：向用户提供可靠的端到端（end to end）服务。传输层向高层屏蔽了下层数据通信的细节，因此，它是计算机通信体系结构中关键的一层。

5. 会话层

在 OSI 参考模型中，会话层（Session Layer）是参考模型的第 5 层。会话层的主要功能是：负责维护两个节点之间会话连接的建立、管理和终止，以及数据的交换。

6. 表示层

在 OSI 参考模型中，表示层（Presentation Layer）是参考模型的第 6 层。表示层的主要功能是：用于处理在两个通信系统中交换信息的表示方式，主要包括数据格式变换、数据加密与解密、数据压缩与恢复等功能。

7. 应用层

在 OSI 参考模型中，应用层（Application Layer）是参考模型的最高层。应用层的主要功能是：为应用程序提供网络服务。应用层需要识别并保证通信对方的可用性，使得协同工作的应用程序之间的同步，建立传输错误纠正与保证数据完整性控制机制。

OSI 只是一个参考模型，做了一些原则性的说明，而不是一个具体的网络。尽管一些具体的网络产品或协议都能在 OSI 模型中找到对应关系，但并不完全相同。

二、局域网参考模型

与 OSI 参考模型比较，局域网协议应该包括 OSI 低三层，即物理层、数据链路层和网络层。但由于在局域网中没有路由问题，任意两点之间可用一条直接的链路而不需要单独设置网络层，因此可将寻址、排序、流量控制和差错控制等功能放在数据链路层中去实现。图 1－4 示出了局域网与 OSI 模型之间的对应关系。

1. 物理层

与 OSI 的物理层接口功能一样，主要包括物理接口的电气特性、连接器和传输媒体的机械特性、接口电路及其功能、信号方式和速率等。

2. 数据链路层

局域网体系结构的数据链路层由介质访问控制（MAC）子层和逻辑链路控制（LLC）子层构成。其中的介质访问控制子层的主要功能是控制对传输介质的访问，对不同类型的局域网需要采用不同的控制方法；逻辑链路控制子层的主要功能是建立和释放数据链路层的逻辑连接，提供与高层的接口、进行差错控制和给帧编号。逻辑链路控制可以提供两种控制类型：无连接服务和面向连接服务。

局域网的大多数标准都是由 IEEE 802 委员会制定的。IEEE（国际电气电子工程师协会）是世界上最大的专业组织之一，该组织于 1980 年成立了局域网标准化委员会（即 IEEE 802 委员会）。该委员会针对各种不同的局域网结构制定了一系列的标准，如适用于总线形局域网的 802.3 协议、适用于环形局域网的 802.5 协议等等。它们统称为 IEEE 802 协议。

图 1－4　局域网与 OSI 模型之间的对应关系